

## **BAB V**

### **KESIMPULAN DAN SARAN**

#### **1.1 Kesimpulan**

Setelah melakukan penelitian mengenai implementasi keamanan *file citra bitmap* pada *private cloud* dengan enkripsi dan dekripsi Algoritma AES-256 CBC maka dapat diambil beberapa kesimpulan yang selaras dengan tujuan penelitian. Berikut beberapa kesimpulan yang didapat oleh penulis.

1. Penelitian ini berhasil merancang Implementasi Kriptografi untuk verifikasi dan pengamanan data yang aman untuk *File Citra Bitmap* di *Private Cloud*.
2. Penelitian ini berhasil mengimplementasikan AES-256 CBC saat *user* akan mengupload *File Citra Bitmap*. Verifikasi adalah dengan adanya fungsi untuk mendeteksi gambar sama atau tidak di database *Cloud Storage*. Pengamanan data dengan enkripsi AES-256 CBC.
3. Penelitian ini berhasil melakukan pengujian sebagai berikut
  - Pengujian waktu eksekusi dari ukuran dimensi file citra bitmap, semakin besar dimensi piksel yang dimiliki semakin lama waktunya. Ukuran filenya semakin besar dan sangat aman.
  - Pengujian hasil enkripsi dari implementasi dan di uji pada *webtool online encryption* telah berhasil enkripsi tidak bisa di decrypt. Sehingga berkesimpulan enkripsi aman.
  - Pengujian dan hasil analisis memenuhi empat unsur keamanan dalam Kriptografi.

#### **1.2 Saran**

Dalam pelaksanaan penelitian, penulis menyadari bahwa masih banyak kekurangan yang dilakukan oleh penulis dalam penelitian ini, oleh karena itu, penulis menyampaikan beberapa saran yang dapat dilakukan oleh peneliti selanjutnya di kemudian hari. Penelitian selanjutnya dapat menghasilkan sebuah program yang jauh lebih baik dalam hal memperbanyak metode atau teknik. Berikut beberapa saran yang dapat oleh penulis anjurkan.

1. Mengefisiensikan kode program AES-256 CBC untuk dalam komputasi.

2. Citra yang digunakan bisa lebih dari 1 MegaBytes.
3. Menggunakan metode enkripsi pesan rahasia lebih kuat lagi agar keamanan pesan rahasia dapat lebih terjaga keamanannya.
4. Penulis harap program ini dapat menjadi modal awal dalam melakukan penelitian – penelitian selanjutnya dengan menggunakan studi kasus yang memerlukan teknik AES-256 CBC pada *Private Cloud*.